# McAfee® Email Security Appliance (VMtrial) Version 5.6

Installationshandbuch

## COPYRIGHT

Copyright © 2011 McAfee, Inc. Alle Rechte vorbehalten.

Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übermittelt, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

## MARKEN

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD sind eingetragene Marken oder Marken von McAfee, Inc. und/oder der Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum der jeweiligen Besitzer.

## INFORMATIONEN ZUR LIZENZ

### Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

# Inhaltsverzeichnis


**Einführung in VMtrial** . . . . . **5**

Funktionen . . . . . 5

Testzeitraum . . . . . 9

Leistung . . . . . 9

Zielgruppe . . . . . 9

Informationen zu McAfee . . . . . 9

Informationen zu VMware . . . . . 10

Was Sie bekommen . . . . . 10

Was geschieht, wenn der Testzeitraum abläuft? . . . . . 11

**Installieren von VMtrial** . . . . . **12**

Entscheiden, wie Sie den Testzeitraum nutzen möchten . . . . . 12

Überlegungen vor der Installation von VMtrial . . . . . 12

Benötigte Netzwerkangaben . . . . . 13

Systemanforderungen . . . . . 13

Installationsschritte . . . . . 13

Installieren von VMware Server 2.0 . . . . . 14

Installieren der Virtual Appliance . . . . . 14

Konfigurieren der Netzwerkeinstellungen . . . . . 16

Alternative Installationsoptionen . . . . . 16

Installieren von VMware Server 1.0 . . . . . 16

Ausführen der VMX-Datei auf VMware Server 1.0 . . . . . 17

Installation von VMware Server 1.0 und VMware Server 2.0 unter Linux . . . . . 18

**Erste Schritte mit VMtrial** . . . . . **20**

Die Benutzeroberfläche . . . . . 20

Dashboard-Statusinformationen und Konfigurationsoptionen . . . . . 22

Testen der Konfiguration . . . . . 27

Testen der Verbindung . . . . . 27

Aktualisieren der DAT-Dateien . . . . . 27

Testen von E-Mail-Verkehr und Virenerkennung . . . . . 28

Testen der Spam-Erkennung . . . . . 28

Erkunden der VMtrial-Funktionen . . . . . 29

Scan-Richtlinien und deren Einfluss auf Ihr Netzwerk. . . . . 29
Inhaltsscans unter Verwendung der E-Mail-Compliance-Regeln. . . . . 29
Vermeiden des Verlusts vertraulicher Daten. . . . . 31
Bearbeiten von isolierten Nachrichten. . . . . 32
Überwachen der Spam-Erkennung. . . . . 32
Ausführen von VMtrial auf dem VMware Server im Betriebsmodus "Transparent". . . . . 33

# Einführung in VMtrial

McAfee® Email Security Appliance (VMtrial) ermöglicht Ihnen, die neueste Email Security Appliance auf den folgenden virtuellen VMware-Plattformen zu testen:

- VMware ESXi
- VMware ESX
- VMware Server

Die Email Security Appliance liefert umfassenden Schutz für Unternehmen vor Web-Bedrohungen in einer integrierten und benutzerfreundlichen Appliance für die folgenden Protokolle:

- SMTP
- POP3

Wenn Sie die Email Security Appliance nach Ablauf des Tests erwerben, kann McAfee Ihnen die entsprechende Hardware und andere Artikel liefern, die im Lieferumfang einer Appliance enthalten sind, oder Sie können über einen virtuellen Server auf die Software zugreifen.

**Inhalt**


- Funktionen
- Testzeitraum
- Leistung
- Zielgruppe
- Informationen zu McAfee
- Informationen zu VMware
- Was Sie bekommen
- Was geschieht, wenn der Testzeitraum abläuft?


# Funktionen

Diese Informationen beschreiben die Funktionen der McAfee Email Security Appliance (VMtrial) sowie deren Position in der Produktoberfläche:

- Tabelle 1: E-Mail-Scan-Funktionen

- Tabelle 2: Berichterstellungs- und Systemfunktionen

HINWEIS: Im weiteren Verlauf dieses Dokuments finden Sie für einige Funktionen Hinweise zur Verwendung.

Tabelle 1: E-Mail-Scan-Funktionen

| Funktion | Beschreibung |
|---|---|
| **Umfassender Scan-Schutz** | Die Email Security Appliance (VMtrial) bietet Antiviren- und Anti-Spam-Schutz für die folgenden Netzwerkprotokolle:<br>• SMTP<br>• POP3 |
| **Antiviren-Schutz** | **E-Mail \| E-Mail-Richtlinien \| Scan-Richtlinien \| [Anti-Virus]**<br>Reduzierung der Bedrohungen für den gesamten Protokollverkehr durch folgende Mittel:<br>• Virenschutzeinstellungen zur Identifizierung bekannter und unbekannter Bedrohungen von Viren in Archivdateien und anderen Dateitypen.<br>• Weitere Einstellungen für die Bedrohungserkennung zum Erkennen von Viren, potentiell unerwünschten Programmen, Komprimierungsprogrammen und anderer Malware.<br>• **Datei-Reputation von McAfee Global Threat Intelligence** zur Ergänzung der DAT-basierten Signaturen, indem den Appliances der Zugriff auf Millionen von Cloud-basierten Signaturen ermöglicht wird. Dadurch wird die Zeitspanne zwischen der Entdeckung einer neuen Malware durch McAfee und deren Aufnahme in die DAT-Dateien reduziert, was den Schutz erhöht. |
| **Anti-Spam-Schutz** | **E-Mail \| E-Mail-Richtlinien \| Scan-Richtlinien \| [Spam]**<br>Verringert Spam in SMTP- und POP3-E-Mail-Verkehr durch folgende Mittel:<br>• Anti-Spam-Modul, Anti-Spam- und Anti-Phishing-Regelsätze.<br>• Listen zugelassener und nicht zugelassener Absender<br>• **E-Mail-Reputation von McAfee Global Threat Intelligence** zur Identifizierung von Absendern von Spam-E-Mails.<br>• Einschluss- und Ausschlusslisten, die Administratoren und Benutzer mithilfe eines Microsoft Outlook-Plugins (nur auf Benutzerebene) erstellen können.<br>Erkennt Phishing-Angriffe und ergreift die entsprechenden Maßnahmen. |
| **McAfee Global Threat Intelligence-Feedback** | **E-Mail \| E-Mail-Richtlinien \| Scan-Richtlinien \| McAfee GTI-Feedback**<br>**System \| Setup-Assistent \| Datenverkehr**<br>McAfee analysiert die Daten über Produkterkennungen und -warnmeldungen, Bedrohungsdetails und Nutzerstatistiken von einem vielschichtigen Kundenstamm, um wirksam gegen elektronische Angriffe vorzugehen, anfällige Systeme zu schützen und Internetkriminalität abzuwehren. Durch Ihre Teilnahme am Feedback-Dienst helfen Sie uns dabei, McAfee Global Threat Intelligence zu verbessern, sodass Ihre McAfee-Produkte effektiver arbeiten, und unterstützen unsere Zusammenarbeit mit Strafverfolgungsbehörden im Hinblick auf die Bekämpfung elektronischer Bedrohungen. |
| **Compliance-Einstellungen** | **E-Mail \| E-Mail-Richtlinien \| Scan-Richtlinien \| [Compliance]**<br>Diese Version der McAfee Email Security Appliance-Software beinhaltet Verbesserungen hinsichtlich der Art und Weise der Verwendung von Compliance-Regeln:<br>• Verwenden Sie in der **Compliance**-Richtlinie den Assistenten für die Regelerstellung, um die integrierten Wörterbücher für die |

| Funktion | Beschreibung |
|---|---|
| | Compliance-Prüfung festzulegen, oder erstellen Sie eine neue Regel, für die Sie eine vorhandene Regel als Vorlage verwenden können.<br>• Mit den Richtlinien **Mail-Größenfilterung** und **Dateifilterung** können Sie SMTP-E-Mail-Nachrichten auf echte Dateitypen überprüfen und auf der Grundlage der Größe und Anzahl der Anhänge Maßnahmen ergreifen. |
| **Data Loss Prevention** | **E-Mail \| E-Mail-Richtlinien \| Scan-Richtlinien \| [Data Loss Prevention]**<br>Mit der **Data Loss Prevention**-Richtlinie können Sie kritische Dokumente hochladen und analysieren – dies wird als "Training" bezeichnet – und einen Fingerabdruck aller Dokumente erstellen. |
| **Nachrichtensuche** | **E-Mail \| Nachrichtensuche**<br>Mit der Nachrichtensuche können Sie von einer einzigen Stelle der Benutzeroberfläche aus den Status von E-Mails bestätigen, die die Appliance durchlaufen haben. Sie erhalten Informationen zur E-Mail, beispielsweise ob sie zugestellt, blockiert, gebounct, isoliert oder in die Warteschlange für ausstehende weitere Aktionen gestellt wurde. |
| **Quarantänefunktionen** | **E-Mail \| Quarantäne-Konfiguration \| Quarantäneoptionen**<br>• **Quarantäne-Digests** Ermöglichen den Benutzern die Bearbeitung isolierter Elemente ohne Einbeziehung des E-Mail-Administrators.<br>• **McAfee Quarantine Manager** Fasst die Quarantäneverwaltung für McAfee-Produkte zusammen. |
| **Message Transfer Agent** | • Leitet Datenverkehr um, basierend auf Kriterien, die vom Administrator festgelegt werden. Beispielsweise können verschlüsselte E-Mails zur Entschlüsselung umgeleitet werden.<br>• Erlaubt es dem Administrator, den finalen Status jeder Nachricht zu bestimmen.<br>• Zeigt eine Kurzübersicht eingehender E-Mails nach Domänen, mit Detaillierungsmöglichkeiten nach Domäne und nicht zugestellter E-Mail nach Domäne.<br>• Priorisiert die erneute Zustellung nicht zugestellter E-Mails abhängig von der Domäne.<br>• Fasst die Zustellung mehrerer E-Mails an die jeweilige Domäne zusammen.<br>• Erneutes Schreiben von E-Mail-Adressen bei ein- und ausgehender E-Mail auf der Grundlage normaler Ausdrücke, die vom Administrator definiert wurden.<br>• Entfernt E-Mail-Header bei ausgehenden Nachrichten, um den Aufbau der internen Netzwerkinfrastruktur zu verbergen.<br>• Versendet E-Mails unter Verwendung von TLS.<br>• Verwaltet Zertifikate. |

Tabelle 2: Berichterstellungs- und Systemfunktionen

| Funktion | Beschreibung |
|---|---|
| **Geplante Berichte** | **Berichte \| Geplante Berichte**<br>Sie können Berichte planen, die regelmäßig ausgeführt und an einen oder mehrere E-Mail-Empfänger gesendet werden sollen. |
| **Protokollierungsoptionen** | **System \| Protokollierung, Warnung und SNMP**<br>Sie können die Appliance für das Senden von E-Mails, die Informationen zu Viren und anderen erkannten |

| Funktion | Beschreibung |
|---|---|
| | Bedrohungen enthalten, sowie für die Verwendung von SNMP zum Übertragen von Informationen von der Appliance konfigurieren. |
| **Dashboard-Statistiken** | **Dashboard**<br>Das Dashboard bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Aktivitäten der Appliance ansehen können, wie beispielsweise von der Appliance verarbeitete E-Mails und den Gesamtsystemstatus der Appliance. Sie können auch eine Liste von Links zu Aufgaben konfigurieren, die Sie häufig verwenden. |
| **Verwalten von Appliances über ePolicy Orchestrator** | **System \| Setup-Assistent \| Einrichten der Verwaltung durch ePO**<br>Sie können in ePolicy Orchestrator den Status Ihrer Appliances überwachen und sie verwalten.<br>Sie können die Appliances direkt über ePolicy Orchestrator verwalten, ohne die Benutzeroberfläche für jede Appliance starten zu müssen.<br>In ePolicy Orchestrator ähneln die Seiten der Benutzeroberfläche, die Sie zum Konfigurieren und Verwalten Ihrer Email Security Appliances verwenden, hinsichtlich ihrer Gestaltung den Seiten, die Sie von den Appliances gewohnt sind. |
| **Cluster-Verwaltung** | **System \| Cluster-Verwaltung**<br>Die Cluster-Verwaltung ermöglicht Ihnen, Gruppen von zusammenarbeitenden Appliances einzurichten, um die Scan-Arbeitslast zu verteilen und für den Fall eines Hardware-Fehlers Redundanz zu bieten.<br>Auf diesen Seiten können Sie Ihre Konfigurationen sichern und wiederherstellen, Konfigurationen von einer Appliance auf andere Appliances übertragen und den Lastenausgleich zwischen den Appliances einrichten. |
| **Virtuelle Hosts** | **System \| Virtuelles Hosting \| Virtuelle Hosts**<br>Für das SMTP-Protokoll können Sie im Adresspool für eingehenden Datenverkehr die Adressen angeben, an denen die Appliance Datenverkehr empfängt oder abfängt.<br>Unter Verwendung virtueller Hosts kann eine einzelne Appliance sich wie verschiedene Appliances verhalten. Jede virtuelle Appliance kann Datenverkehr innerhalb angegebener IP-Adresspools verwalten, wodurch die Appliance Scan-Dienste für Datenverkehr von zahlreichen Kunden bieten kann. |
| **Rollenbasierte Zugriffskontrolle** | **System \| Benutzer, Gruppen und Dienste \| Rollenbasierte Benutzerkonten**<br>Zusätzlich zur Kerberos-Authentifizierungsmethode steht auch die RADIUS-Authentifizierung zur Verfügung. |
| **Internes Rescue-Image** | **System \| Appliance-Verwaltung \| Systemverwaltung \| Internes Rescue-Image verwalten**<br>Wenn Sie Ihre Email Security Appliances verwalten, können Sie, wenn das Image für jede Appliance auf einer geschützten Partition auf der Festplatte für jede Appliance gespeichert ist, remote ein neues Image Ihrer Appliances einspielen. |

| Funktion | Beschreibung |
|---|---|
| | Durch das Rescue-Image entfällt die Notwendigkeit, Ihre Appliance mit Karten für den Remote-Zugriff auszustatten (sofern Sie geeignete Appliance-Modelle verwenden), um von einem Remote-Standort aus ein neues Image auf die Appliances einzuspielen.<br>Zusätzlich zur Installation des Software-Images auf der geschützten Partition können Sie auch auf einem USB-Laufwerk ein bootfähiges Image für Ihre Appliances erstellen. |

# Testzeitraum

*Der Testzeitraum beträgt 30 Tage*, anschließend kann die virtuelle Appliance nicht mehr ausgeführt werden.

Während des Testzeitraums erhalten Sie unbegrenzten Zugriff auf die Funktionen der Email Security Appliance, die Ihre Firma vor Spam, Phishing, Viren, unerwünschten Inhalten, Datenverlust und anderen Bedrohungen schützen können. Siehe Funktionen.

# Leistung

Das Verwenden der virtuellen VMware Server-Appliance zur Simulation einer McAfee-Appliance hat Auswirkungen auf die Leistung der Appliance und den Datendurchsatz. Der Scan-Durchsatz während des Testzeitraums ist nicht repräsentativ für die Leistung, die auf einer McAfee-Appliance mit einer ähnlichen Hardware-Spezifikation erzielt würde. Die Leistung und der Datendurchsatz werden auch von der Spezifikation des Host-Computers und der Geschwindigkeit Ihres Internetanschlusses beeinflusst.

HINWEIS: VMtrial wurde für die Ausführung auf Computern unter VMware Server, die mit einer einzigen CPU konfiguriert wurden, optimiert.

# Zielgruppe

Typischerweise werden diese Appliances von Netzwerkadministratoren verwendet, die für die E-Mail- und Netzwerksicherheit ihrer Firma verantwortlich sind, und von Prüfern, die Email Security Appliance-Produkte testen. Email Security Appliance (VMtrial) ermöglicht es an McAfee-Appliances interessierten Personen, eine voll funktionsfähige Email Security Appliance in einer virtuellen Umgebung zu testen.

# Informationen zu McAfee

McAfee, Inc., mit Hauptsitz in Santa Clara, Kalifornien, ist das weltweit größte, auf Sicherheitstechnologie spezialisierte Unternehmen. Das Unternehmen hat sich der Beantwortung anspruchsvollster Sicherheitsherausforderungen verschrieben. Seinen Kunden liefert McAfee präventive, praxiserprobte Lösungen und Dienstleistungen, die Computer und ITK-Netze auf der ganzen Welt vor Angriffen schützen und es Anwendern ermöglichen, gefahrlos Verbindung mit dem Internet aufzunehmen und sich im World Wide Web zu bewegen. Unterstützt von einer

preisgekrönten Forschungsabteilung, entwickelt McAfee innovative Produkte, die Privatnutzern, Firmen, Behörden und Serviceanbietern helfen, ihre Daten zu schützen, einschlägige Gesetze einzuhalten, Störungen zu verhindern, Schwachstellen zu ermitteln und die Sicherheit ihrer Systeme laufend zu überwachen und zu verbessern. Weitere Informationen über McAfee finden Sie unter http://www.mcafee.com

# Informationen zu VMware

VMware® (NYSE: VMW) bietet Lösungen für die Virtualisierung und Cloud-Infrastruktur, mit denen IT-Organisationen Unternehmen aller Größen ausstatten können. Kunden vertrauen der führenden Virtualisierungsplattform VMware vSphere™, um Investitionen und laufende Ausgaben einzusparen, Business Continuity zu garantieren, ein höheres Sicherheitsniveau zu erreichen und ökologische Ziele wie Energieeinsparung umzusetzen Mit mehr als 190.000 Kunden, über 25.000 Partnern und einem Umsatz von 2 Milliarden US-Dollar in 2009 ist VMware weltweiter Marktführer für Virtualisierung, das Thema mit fortwährend oberster Priorität für CIOs. VMware hat seinen Hauptsitz in Silicon Valley und ist weltweit mit Niederlassungen vertreten. Die Internetadresse lautet: http://www.vmware.com.

# Was Sie bekommen

In der Test-ZIP-Datei finden Sie die folgenden Elemente:

- VMware Server Virtual Appliance
- Installationsdateien der Email Security Appliance
- *Email Security Appliance (VMtrial) Installationshandbuch*

## Informationsquellen

- **Online-Hilfe**
  - Die Konfigurationskonsole enthält seitenbezogene Hilfeinformationen, die Sie beim Installationsvorgang unterstützen.
  - Nach der Installation kann über die Benutzeroberfläche des Produkts eine ausführliche kontextbezogene Hilfe mit **Such-** und **Indexfunktionen** aufgerufen werden. Sie bietet eine Einführung in das Produkt und seine Funktionen, detaillierte Anweisungen zur Konfiguration der Software sowie Informationen zu wiederkehrenden Aufgaben und Betriebsverfahren.
- **KnowledgeBase**: In der McAfee KnowledgeBase finden Sie Antworten auf Fragen zur Email Security Appliance.

  Besuchen Sie die Seite https://mysupport.mcafee.com/, und klicken Sie auf **Browse the KnowledgeBase** (KnowledgeBase durchsuchen). Wählen Sie in der Liste **Product** (Produkt) **Email Security Appliance-Software**.
- **Documentation** (Dokumentation): Sie haben Zugriff auf die neueste Version der Dokumentation für Email Security Appliance.

  Navigieren Sie zu https://mysupport.mcafee.com/, klicken Sie auf **Product Documentation** (Produktdokumentation), und wählen Sie **Email Security Appliance-Software**.

HINWEIS: Hilfe zu VMware Server erhalten Sie unter http://www.vmware.com. Klicken Sie in der Link-Leiste auf **Support & Downloads**, und wählen Sie **KnowledgeBase**.

# Was geschieht, wenn der Testzeitraum abläuft?

Wenn der Testzeitraum endet, wird im Dialogfeld **Ablaufinformationen** auf der VMtrial-Anmeldeseite die Meldung "Der Testzeitraum ist jetzt abgelaufen" angezeigt. Keine der Funktionen von Email Security Appliance (VMtrial) ist mehr aktiv. Der Verkehr passiert weiterhin die VMtrial-Appliance, wird aber nicht gescannt.

HINWEIS: Wenn Sie keine Zeit mehr haben, Ihre Evaluierung abzuschließen, bevor der Testzeitraum abläuft, können Sie Ihre Konfiguration speichern, eine andere Evaluierung starten und Ihre ursprünglichen Konfigurationsienstellungen übernehmen.

Setzen Sie sich mit Ihrem bevorzugten Händler in Verbindung, wenn Sie das Produkt auf der Grundlage Ihrer Evaluierung erwerben möchten. Um einen Händler zu finden, gehen Sie zu http://www.mcafee.com, und suchen Sie nach einem Händler oder Vertriebspartner, oder setzen Sie sich mit einem Vertriebsmitarbeiter in Verbindung.

# Installieren von VMtrial

Diese Informationen helfen Ihnen dabei, Ihre Testumgebung vorzubereiten, und machen Sie auf Themen aufmerksam, die Sie vor der Installaion von Email Security Appliance (VMtrial) bedenken sollten.

**Inhalt**


- Entscheiden, wie Sie den Testzeitraum nutzen möchten
- Überlegungen vor der Installation von VMtrial
- Benötigte Netzwerkangaben
- Systemanforderungen
- Installationsschritte
- Alternative Installationsoptionen


# Entscheiden, wie Sie den Testzeitraum nutzen möchten

Entscheiden, ob Sie:

- Email Security Appliance (VMtrial) zum Scannen von E-Mail-Verkehr in Ihrem Netzwerk verwenden möchten.
- Einfach die Funktionen und Schnittstellenoptionen von Email Security Appliance evaluieren möchten.

# Überlegungen vor der Installation von VMtrial

Wenn die Email Security Appliance den E-Mail- und Web-Verkehr in Ihrem Netzwerk scannen soll, sollten Sie Folgendes vor der Installation bedenken:

- Welche und wie viele Firewalls oder Router werden verwendet?
- Welcher Typ von Netzwerk-Switch wird verwendet?
- Handelt es sich um einen nicht verwalteten Switch der Schicht 2 oder einen verwalteten Switch der Schicht 3 mit einem Routing-Modul?
- Welche Protokolle sollen gescannt werden? Wählen Sie zwischen SMTP und POP3.
- Sollen diese Protokolle gescannt werden, ohne dass Einstellungen auf Clients oder Servern geändert werden?
- Verfügt Ihr Netzwerk über eine DMZ? Falls ja, welche Server befinden sich darin?
- Haben Sie einen internen DNS-Server?

- Haben Sie Remote-Einwahl- oder VPN-Benutzer?

# Benötigte Netzwerkangaben

Ermitteln Sie die folgenden Informationen, um die Konfigurationskonsole ausfüllen zu können:

- Zu scannende Protokolle (SMTP, POP3)
- Host-Name
- Domänenname
- Standard-Gateway
- Wählen Sie den Betriebsmodus aus: Expliziter Proxy, Transparenter Router, Transparente Bridge
- IP-Adresse und Subnetzmaske des LAN1-Anschlusses
- IP-Adresse und Subnetzmaske des LAN2-Anschlusses
- IP-Adresse des DNS-Servers

# Systemanforderungen

In diesem Dokument wird davon ausgegangen, dass Sie für den Test einen Microsoft Windows-Computer verwenden.

Die Oberfläche der Appliance ist für Microsoft Internet Explorer 7.0 oder höher und Mozilla Firefox 3.6 oder höher optimiert.

Wenn Sie planen, VMtrial in Ihrer Produktionsumgebung zu verwenden, denken Sie daran, dass der Datendurchsatz und die Leistung geringer sind als bei einer Appliance mit einer ähnlichen Hardware-Spezifikation.

HINWEIS: VMtrial kann nicht im FAT32-Dateisystem ausgeführt werden.

Tabelle 3: Systemanforderungen

| Komponente | Wert |
|---|---|
| Prozessor | Pentium 4-Prozessor mit 2,8 GHz und Unterstützung für Physical Address Extension (PAE) |
| Betriebssystem | 32-Bit-Microsoft Windows, Linux |
| Verfügbarer Speicher | 1 GB |
| Freier Festplattenspeicher | 50 GB |

# Installationsschritte

Für die Installation von Email Security Appliance (VMtrial) sind drei Schritte notwendig:

1. Installieren von VMware Server 2.0
2. Installieren der Virtual Appliance
3. Konfigurieren der Netzwerkeinstellungen

# Installieren von VMware Server 2.0

Gehen Sie wie nachfolgend beschrieben vor, um VMware Server 2.0 in einer Microsoft Windows-Umgebung auf dem Computer zu installieren, auf dem Sie VMtrial ausführen möchten. Sie können ihn auch in einer Linux-Umgebung installieren. Siehe Installation von VMware Server 1.0 und VMware Server 2.0 unter Linux.

VMtrial kann auch erfolgreich mit VMware Server 1.0, VMware ESX 3.5 und höher und VMware ESXi ausgeführt werden.

Weitere Informationen zu VMware Server erhalten Sie unter http://www.vmware.com/products/server/.

HINWEIS: Die Installation kann etwa 20 Minuten dauern.

### Vorgehensweise

1. Melden Sie sich als Administrator am Computer an.
2. Öffnen Sie das Installationspaket von VMware Server:
   - Doppelklicken Sie unter Microsoft Windows XP auf die EXE-Datei.
   - Klicken Sie unter Microsoft Windows Vista mit der rechten Maustaste auf die EXE-Datei, und wählen Sie **Als Administrator ausführen**.

   Warten Sie nun, bis VMware Server 2.0 dekomprimiert wird und der Windows Installer startet.
3. Klicken Sie im Installationsassistenten von VMware Server auf der Seite **Welcome** (Willkommen) auf **Next** (Weiter).
4. Stimmen Sie den Lizenzbedingungen zu, und klicken Sie auf **Next** (Weiter).
5. Behalten Sie im **Destination Folder** (Zielordner) den standardmäßigen Installationsort bei, oder klicken Sie auf **Change** (Ändern), um einen neuen auszuwählen. Klicken Sie auf **Next** (Weiter).
6. Geben Sie unter **Server Configuration Information** (Serverkonfigurationsinformationen) den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Host-Computers ein. Dabei können im Normalfall die Standard-Ports beibehalten werden. Klicken Sie auf **Next** (Weiter).
7. Wählen Sie in **Configure Shortcuts** (Verknüpfungen konfigurieren) die zu verwendenden Verknüpfungssteuerelemente zu VMware Server 2.0 aus. Klicken Sie auf **Next** (Weiter).
8. Klicken Sie auf **Install** (Installieren), und haben Sie ein wenig Geduld, während VMware Server installiert wird.
9. Gehen Sie auf die VMware-Website, und holen Sie sich einen Lizenzschlüssel für VMware Server 2.0.
10. Geben Sie den Lizenzschlüssel für VMware Server ein, falls sich nicht bereits einer auf dem Computer befindet.
11. Optional können Sie nun noch Ihre Installation registrieren. Die Seriennummer entspricht dem Lizenzschlüssel.
12. Klicken Sie auf **Finish** (Fertig stellen).

# Installieren der Virtual Appliance

Gehen Sie wie nachfolgend beschrieben vor, um die Email Security Appliance-Software mithilfe der VMX-Datei auf VMware Server 2.0 zu installieren.

## Vorgehensweise

1. Öffnen Sie die VMware Infrastructure Web Access-Konsole (**Start | VMware | VMware Server Home Page**) (Start | VMware | VMware Server-Homepage).
2. Melden Sie sich mit Ihrem Microsoft Windows-Anmeldenamen und -Kennwort an.
3. Klicken Sie in **Commands** (Befehle) auf **Add Datastore** (Datenspeicher hinzufügen), und geben Sie einen Namen dafür ein. Geben Sie den gesamten Verzeichnispfad ein, in den Sie zuvor die VMX-Datei extrahiert haben, und klicken Sie auf **OK**.
4. Halten Sie den VMware-DHCP-Server an, um eine Störung des DHCP-Servers in Ihrem Netzwerk zu vermeiden.
   a. Öffnen Sie die Virtual Network Editor-Konsole (**Start | VMware | VMware Server | Manage Virtual Networks**) (Start | VMware | VMware Server | Virtuelle Netzwerke verwalten). Wenn Sie das Betriebssystem Microsoft Windows Vista verwenden, klicken Sie mit der rechten Maustaste auf **Manage Virtual Networks** (Virtuelle Netzwerke verwalten), und wählen Sie **Run as administrator** (Als Administrator ausführen).
   b. Klicken Sie auf die Registerkarte **DHCP**.
   c. Klicken Sie auf **Stop** (Anhalten) und anschließend auf **OK**.
5. Fügen Sie VMtrial als Virtual Machine hinzu:
   a. Wählen Sie in VMware Infrastructure Web Access im Bereich **Commands** (Befehle) **Add Virtual Machine to Inventory** (Virtuelle Maschine zu Inventar hinzufügen) und anschließend den Datenspeicher, den Sie zuvor erstellt haben.
   b. Wählen Sie die VMX-Datei von McAfee in der Liste **Contents** (Inhalt), und klicken Sie auf **OK**. Anschließend sollte die Datei in der Liste **Inventory** (Inventar) zu sehen sein.
6. Stellen Sie die Hardware-Optionen so ein, dass die VMtrial entweder auf Ihrem Netzwerk ausgeführt wird, um den Datenverkehr zu scannen, oder auf dem Host-Computer.

   HINWEIS: Um Netzwerk-Loops bei VMtrial im Modus "Nur Host" zu vermeiden, empfiehlt McAfee, dass Sie den Modus "Transparente Bridge" *nicht* ausführen.

   a. Wählen Sie in der VMware Infrastructure Web Access-Konsole die virtuelle Maschine aus.
   b. Wählen Sie in der Liste **Hardware** (Hardware) **Network Adapter 1** (Netzwerkadapter 1), und klicken Sie auf **Edit** (Bearbeiten). Ändern Sie die Hardware-Optionen Ihren Anforderungen entsprechend. Wiederholen Sie den Vorgang für Network Adapter 2 (Netzwerkadapter 2).
   c. Klicken Sie auf **OK**.
7. Wählen Sie in VMware Infrastructure Web Access die virtuelle Maschine von VMtrial aus, und klicken Sie auf die grüne Schaltfläche, um sie zu starten.
8. Ansicht der Konsole der Virtual Machine:
   a. Wählen Sie in VMware Infrastructure Web Access **Console** (Konsole), und klicken Sie anschließend auf eine beliebige Stelle in dem schwarzen Fenster. Eventuell werden Sie gebeten, bei der ersten Installation das Konsolen-Plug-in für VMware Remote Access zu installieren.
   b. Akzeptieren Sie die Lizenzvereinbarung.
   c. Wählen Sie **Option 1**.
   d. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie fortfahren möchten, und warten Sie, bis die Email Security Appliance (VMtrial) installiert ist. Die Konfigurationskonsole von VMtrial wird angezeigt.

## Konfigurieren der Netzwerkeinstellungen

Die Konfigurationskonsole wird am Ende der Startsequenz automatisch gestartet, entweder nachdem:

- ein unkonfiguriertes Gerät gestartet wurde
- oder nachdem ein Gerät auf seine Werkseinstellungen zurückgesetzt wurde.

Wird die Konfigurationskonsole gestartet, bietet Sie Ihnen die Möglichkeit, Ihr Gerät von der Gerätekonsole aus in Ihrer bevorzugten Sprache zu konfigurieren, bzw. liefert Anweisungen dafür, wie Sie von einem anderen Computer im selben Klasse-C-Subnetz aus eine Verbindung mit dem Setup-Assistenten innerhalb der Benutzeroberfläche (**System | Setup-Assistent**) herstellen können. Beide Methoden bieten Ihnen dieselben Optionen für die Konfiguration Ihres Geräts.

VMtrial führt für folgende Parameter die automatische Konfiguration mithilfe von DHCP durch:

- Host-Name
- Domänenname
- Standard-Gateway
- DNS-Server

Nachdem Sie alle Informationen eingegeben haben, müssen Sie die Konfiguration übernehmen. Je nach den angegebenen Einstellungen kann es sein, dass die Evaluierungssitzung neu gestartet wird. Die Konsole wird so lange beim Neustart der Appliance angezeigt, bis Sie die Einstellungen festgelegt haben.

HINWEIS: Sie müssen mindestens die LAN1-IP-Adressinformationen festlegen.

# Alternative Installationsoptionen

Im Folgenden finden Sie weitere Konfigurationsinformationen.

## Installieren von VMware Server 1.0

Gehen Sie wie nachfolgend beschrieben vor, um VMware Server 1.0 zu installieren.

Installieren Sie VMware Server auf dem Computer, auf dem Sie VMtrial ausführen möchten. Er steht steht unter http://www.vmware.com zur Verfügung.

Um weitere Informationen zu VMware Server zu erhalten, gehen Sie zu http://www.vmware.com/products/server/.

HINWEIS: Die Installation kann etwa 20 Minuten dauern.

### Vorgehensweise

1. Melden Sie sich als Administrator am Computer an.
2. Öffnen Sie die ZIP-Installationsdatei für VMware Server, und *extrahieren Sie die Inhalte auf die Festplatte des Host-Computers.*
3. Doppelklicken Sie auf die EXE-Datei, und klicken Sie auf **Run** (Ausführen), um die Installation zu starten.
4. Klicken Sie im VMware Server-Installationsassistenten auf **Next** (Weiter), um fortzufahren.
5. Akzeptieren Sie die Lizenzvereinbarung.

6 Behalten Sie unter **Setup Type** (Setup-Typ) die Standardoption **Complete** (Vollständig) bei.

HINWEIS: Möglicherweise sehen Sie einen Hinweis, der besagt, dass die Microsoft Internet Information Services (IIS) nicht installiert sind. Sie benötigen IIS auf dem Host-Computer, wenn Sie die VMware Management-Oberfläche verwenden möchten. Um IIS zu installieren, brechen Sie die Installation nun ab, installieren Sie IIS, und nehmen Sie dann das Setup wieder auf.

7 Behalten Sie im **Destination Folder** (Zielordner) den standardmäßigen Installationsort bei, oder klicken Sie auf **Change** (Ändern), um einen neuen auszuwählen.

8 Klicken Sie auf **Install** (Installieren). Es kann einige Minuten dauern, bis die VMware Server-Komponenten installiert sind.

9 Besuchen Sie http://www.vmware.com, um sich als VMware Server-Benutzer zu registrieren und einen Lizenzschlüssel zu erhalten. Vergewissern Sie sich, dass Sie sich den Lizenzschlüssel notieren.

10 Geben Sie unter **Customer Information** (Kundeninformationen) Ihren Namen, Ihre Organisation und den Lizenzschlüssel ein, und klicken Sie dann auf **Enter** (Eingabe).

11 Klicken Sie auf **Finish** (Fertig stellen).

# Ausführen der VMX-Datei auf VMware Server 1.0

Gehen Sie wie nachfolgend beschrieben vor, um die VMX-Installationsdatei unter VMware Server 1.0 auszuführen und VMtrial zu starten.

### Vorgehensweise

1 Navigieren Sie auf dem Host-Computer *zu dem Speicherort, an den Sie die Inhalte der ZIP-Datei für die Evaluierung extrahiert haben.*

2 Öffnen Sie den Ordner **McAfee-EWS-SMG-5.6....**, der die Installationsdateien für die Email Security Appliance (VMtrial) enthält.

3 Doppelklicken Sie auf die Konfigurationsdatei **EWS-SMG-5.6<Paket-Nummer>.vmx**.

4 Bestätigen Sie, dass Sie die Datei öffnen möchten.

Die VMware Server-Konsole wird gestartet, standardmäßig im Modus **Bridged** (Bridge).

5 Wählen Sie aus der Liste **Inventory** (Inventar) das Element **MWS...** aus.

6 Legen Sie fest, wie VMtrial ausgeführt werden soll:

- **On your network** (In Ihrem Netzwerk) – Wenn VMtrial den E-Mail-Verkehr in Ihrem Netzwerk scannen soll, belassen Sie das Ethernet im Modus **Bridged** (Bridge) (der Standardeinstellung).
- **To share a private network with the host** (Privates Netzwerk, das mit einem Host geteilt wird) – Als privates Netzwerk mit dem Host müssen Sie das Ethernet so einstellen, dass es im Modus **Host-only** (Nur Host) betrieben wird, und Sie müssen die DHCP-Einstellungen prüfen, um den IP-Adressbereich zu erhalten.

HINWEIS: Um Netzwerk-Loops zu vermeiden, empfiehlt McAfee, dass Sie Ihren VMware Server im Modus "Nur Host" ausführen. Führen Sie VMtrial *nicht* im Modus "Transparente Bridge" aus.

**a** Wählen Sie in der VMware Server-Konsole **Edit virtual machine settings** (Einstellungen für virtuelle Maschine bearbeiten).

**b** Legen Sie **Ethernet0** als **Host-Only** (Nur Host) fest. Belassen Sie Ethernet1 im Modus "Bridge".

**c** Klicken Sie auf **OK**.

**d** Wählen Sie im Menü **Host** die Option **Virtual Network Settings** (Virtuelle Netzwerkeinstellungen).

**e** Klicken Sie im Virtual Network Editor auf die Registerkarte **DHCP**, und notieren Sie sich den IP-Adressbereich. Sie benötigen den IP-Adressbereich später, wenn Sie die Konfigurationskonsole ausfüllen. Sie finden Details zur Auswahl von IP-Adressen für ein "Nur-Host-Netzwerk" in der VMware Server Online Library.

HINWEIS: VMtrial verwendet den DHCP-Dienst von VMware Server nicht. McAfee empfiehlt, dass Sie den DHCP-Dienst von VMware Server deaktivieren, wenn Ihr VMware Server im Modus "Bridge" betrieben wird, und dass Sie eine Adresse aus diesem Bereich für LAN1 der VMtrial-Software festlegen. Verwenden Sie hierfür die VMtrial-Konfigurationskonsole.

Wenn sich ein VMware Server im Modus "Bridge" befindet, kann sein DHCP-Dienst Auswirkungen auf die DHCP-Server in Ihrem Hauptnetzwerk haben.

**7** Wählen Sie in der VMware Server-Konsole **Start this virtual machine** (Diese virtuelle Maschine starten).

**8** Lesen und akzeptieren Sie die Lizenzvereinbarung.

**9** Wählen Sie Option **1**, um einen vollständigen Vorgang auszuführen, und wählen Sie dann **y**, um Ihre Auswahl zu bestätigen. Warten Sie, während VMtrial installiert wird.

Die Konfigurationskonsole wird angezeigt.

# Installation von VMware Server 1.0 und VMware Server 2.0 unter Linux

Gehen Sie wie nachfolgend beschrieben vor, um VMware Server 2.0 oder VMware Server 1.0 auf dem Betriebssystem Linux zu installieren.

## Vorgehensweise

**1** Überprüfen Sie die Kernel-Version Ihres Linux-Systems, und notieren Sie sie.

**2** Stellen Sie sicher, dass die folgenden Pakete auf Ihrem Linux-System installiert sind, bevor Sie VMware Server 2.0 oder VMware Server 1.0 installieren:

- gcc
- Kernel-Header entsprechend der Kernel-Version
- perl

HINWEIS: Es sind möglicherweise auch andere Bibliotheksdateien erforderlich, die gegebenenfalls während der Installation angegeben werden.

**3** Laden Sie die VMware Server-Installationsdatei auf Ihr Linux-System herunter, und extrahieren Sie die TAR-Datei mit tar -xvfz VMware-server-<Versionsnummer>-<Build-Nummer>.tar.gz.

**4** Wechseln Sie in das vmware-server-distrib-Verzeichnis, und führen Sie das Installationsskript ./vmware-install.pl aus.

**5** Folgen Sie den Eingabeaufforderungen in der Befehlszeile.

**6** Geben Sie den Lizenzschlüssel für den VMware Server ein, wenn Sie dazu aufgefordert werden.

# Erste Schritte mit VMtrial

In diesem Abschnitt werden die Elemente der Benutzeroberfläche von Email Security Appliance (VMtrial) vorgestellt.

**Inhalt**


- Die Benutzeroberfläche
- Dashboard-Statusinformationen und Konfigurationsoptionen
- Testen der Konfiguration


# Die Benutzeroberfläche

Verwenden Sie diese Informationen, um die Elemente der Benutzerschnittstelle kennenzulernen.

HINWEIS: Ihre Benutzeroberfläche sieht möglicherweise etwas anders als die in Abbildung 1: Das Dashboard gezeigte Oberfläche aus, da sie aufgrund der Hardware-Plattform, Software-Version und Sprache der Appliance variieren kann.

Die Benutzeroberfläche enthält die folgenden Elemente:

- **Navigationsleiste**

  Die Navigationsleiste umfasst vier Bereiche: Benutzerinformationen, Abschnittssymbole, Registerkartenleiste und Support-Steuerelemente.

- **Benutzerinformationsleiste**
- **Abschnittssymbole**

  Die Anzahl der Abschnittssymbole hängen von der verwendeten Software-Version ab. Klicken Sie auf ein Symbol, um die Informationen im Inhaltsbereich und in der Registerkartenleiste zu ändern. Die folgenden Symbole sind verfügbar:

  Tabelle 4: Abschnittselemente

| Symbol | Menü | Funktionen |
|---|---|---|
| | **Dashboard** | Auf dieser Seite finden Sie eine Übersicht über die Appliance. Von hier aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern. |
| | **Berichte** | Auf den Seiten **Berichte** können Sie Ereignisse sehen, die auf der Appliance aufgezeichnet wurden, wie beispielsweise in E-Mails erkannte Viren und Systemaktivitäten wie etwa Details zu kürzlich erfolgten Aktualisierungen und Anmeldungen. |

| Symbol | Menü | Funktionen |
|---|---|---|
| | **E-Mail** | Mithilfe der Seiten **E-Mail** können Sie Bedrohungen in E-Mails verwalten, infizierte E-Mails isolieren und weitere Aspekte der E-Mail-Konfiguration behandeln. |
| | **System** | Auf den **Systemseiten** können Sie verschiedene Funktionen der Appliance konfigurieren. |
| | **Fehlerbehebung** | Auf den Seiten zur **Fehlerbehebung** können Sie sämtliche Probleme im Zusammenhang mit der Appliance analysieren. |

- **Registerkartenleiste**

  Die Inhalte der Registerkartenleiste werden durch das ausgewählte Abschnittssymbol bestimmt. Die ausgewählte Registerkarte gibt vor, was im Inhaltsbereich angezeigt wird.

- **Support-Steuerungsschaltflächen**

  Die Support-Steuerungsschaltflächen sind Aktionen, die für den Inhaltsbereich gelten.

  Tabelle 5: Support-Steuerungsschaltflächen

| Symbol | Beschreibung |
|---|---|
| | Aktualisiert den Inhalt. |
| | Bringt Sie zur zuvor angezeigten Seite zurück. Es wird empfohlen, auf diese Schaltfläche statt auf die Schaltfläche "Zurück" Ihres Browsers zu klicken. |
| | Dieses Symbol wird angezeigt, wenn Sie etwas konfigurieren, und ermöglicht es Ihnen, Ihre Änderungen anzuwenden. |
| | Dieses Symbol wird angezeigt, wenn Sie etwas konfigurieren, und ermöglicht es Ihnen, Ihre Änderungen zu verwerfen. |
| | Öffnet ein Fenster mit Hilfe-Informationen. Viele der Informationen in diesem Fenster finden Sie auch im Produkthandbuch. |

- **Steuerelemente anzeigen**

  Die Schaltfläche "Steuerelemente anzeigen" blendet ein Statusfenster ein oder aus.

  Das Statusfenster rechts unten in der Benutzeroberfläche zeigt alle kürzlich erfolgten Aktivitäten an. Neue Meldungen werden oben im Fenster hinzugefügt. Wenn eine Meldung blau und unterstrichen ist, können Sie auf den Link klicken, um eine andere Seite zu besuchen. Sie können das Fenster auch über die Links **Leeren** und **Schließen** verwalten.

- **Inhaltsbereich**

  Der Inhaltsbereich enthält den derzeit aktiven Inhalt. Hier findet die meiste Interaktion statt.

HINWEIS: Die vorgenommenen Änderungen werden wirksam, nachdem Sie auf das grüne Häkchen geklickt haben.

# Dashboard-Statusinformationen und Konfigurationsoptionen

Das Dashboard bietet eine Zusammenfassung der Aktivitäten der Appliance.

Von dieser Seite aus können Sie auf die meisten Seiten zugreifen, die die Appliance steuern. Auf einer Cluster-Master-Appliance verwenden Sie diese Seite auch, um eine Übersicht der Aktivitäten im Appliance-Cluster anzuzeigen.

HINWEIS: Wenn Sie die Ansicht in einem Bereich ändern möchten, klicken Sie auf **Bearbeiten**, um ein anderes Fenster zu öffnen.

Das Dashboard bietet einen zentralen Ort, an dem Sie Zusammenfassungen der Aktivitäten der Appliance ansehen können.

Abhängig davon, wie Sie Ihre Appliance konfiguriert haben, können Sie Informationen zu Folgendem ansehen:

- Von der Appliance verarbeitete E-Mails
- Gesamtsystemstatus der Appliance
- Aktuelle Erkennungsraten
- Leistung Ihres Netzwerks
- E-Mail-Nachrichten, die von der Appliance in die Warteschlange gestellt wurden
- Anzahl Ihrer eingerichteten Scan-Richtlinien, nach Protokoll getrennt

Sie können auch eine Liste von Links zu Aufgaben konfigurieren, die Sie häufig verwenden. Dies bietet Ihnen eine schnelle und einfache Methode, um zum richtigen Bereich der Benutzeroberfläche zu navigieren.

Im unteren Bereich dieser Seite werden wichtige grafische Informationen zur Leistung der Appliance angezeigt. Jeder dieser Dashboard-Bereiche kann dahingehend angepasst werden, dass er die Informationen anzeigt, die Sie am häufigsten benötigen.

Wenn Sie sich bei der Appliance anmelden und während der Arbeit auf den Konfigurationsseiten der Appliance wird in der unteren rechten Ecke des Bildschirms ein Dialogfeld angezeigt, das Informationen zu empfohlenen Konfigurationsänderungen oder Warnmeldungen hinsichtlich

des Betriebs oder der Einstellungen der Appliance enthält. Sie werden beispielsweise gewarnt, wenn das Global Threat Intelligence-Feedback nicht für alle Richtlinien aktiviert ist.

Abbildung 1: Das Dashboard

## Bereiche der Seite "Dashboard"

Tabelle 6: Dashboard – Optionsbeschreibungen

| Option | Beschreibung |
|---|---|
| **E-Mail-Erkennungen** | Zeigt die Anzahl der Erkennungen unter jedem Protokoll an. Klicken Sie auf **Bearbeiten**, um die Ansicht in diesem Fenster zu ändern. Obwohl Sie festlegen können, dass zu einem Protokoll keine Informationen angezeigt werden, scannt die Appliance den Verkehr weiterhin. |
| **Systemstatus** | Zeigt den Status wichtiger Komponenten an und ermöglicht Ihnen, Änderungen an den Einstellungen von empfohlenen Systemkonfigurationsänderungen vorzunehmen:<br>• Bei **Aktualisierungen** zeigt ein grünes Häkchen, dass die Komponenten automatisch aktualisiert werden. Wenn Sie eine manuelle Aktualisierung vornehmen möchten, klicken Sie auf den blauen Link.<br>• Für andere Komponenten gibt ein grünes Häkchen an, dass die Komponente innerhalb akzeptabler Grenzwerte betrieben wird. Weiterführende Informationen erhalten Sie, wenn Sie auf die blauen Links klicken.<br>• Sie können die Stufen anpassen, bei denen die Warnhinweissymbole angezeigt werden, und ändern, was im Dialogfeld mit den empfohlenen Konfigurationsänderungen angezeigt wird, indem Sie auf **Bearbeiten** klicken. |
| **Aktuelle Erkennungsraten** | Zeigt mithilfe von Symbolen den Status wichtiger Erkennungen der Appliance an. |
| **Netzwerk** | Zeigt die Anzahl der Verbindungen unter jedem Protokoll an. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten** |

| Option | Beschreibung |
|---|---|
| | abwählen können, wickelt die Appliance den Verkehr weiterhin ab. |
| **E-Mail-Warteschlangen** | Zeigt mithilfe von Symbolen die Anzahl der Elemente und die Anzahl der Empfänger für jedes Element in den Warteschlangen "In der Warteschlange", "Isoliert" und "Anfragen für Entlassen aus Quarantäne" an, die von der Appliance verwaltet werden. Wenn Sie auf die Seiten wechseln möchten, auf denen die Warteschlangen verwaltet werden, klicken Sie auf die blauen Links. Wenn Sie die E-Mails in den Warteschlangen schnell durchsuchen möchten, klicken Sie auf **Schnellsuche**. |
| **Scan-Richtlinien** | Zeigt eine Liste der von der Appliance eingesetzten Richtlinien an. Obwohl Sie ein Protokoll nach Klicken auf **Bearbeiten** abwählen können, wendet die Appliance weiterhin Richtlinien auf den Verkehr an. Wenn Sie die Scan-Richtlinien anzeigen oder weitere Richtlinien hinzufügen möchten, klicken Sie auf die blauen Links. |
| **Tasks** | Zeigt eine Liste häufiger Aufgaben an. Wenn Sie Aufgaben entfernen oder neu organisieren möchten, klicken Sie auf **Bearbeiten**. |
| **Lastenausgleich** | Auf einer Master-Cluster-Appliance wird der Status des Appliance-Clusters angezeigt. Um die Einstellungen der Anzeige zu ändern, klicken Sie auf **Bearbeiten**. |
| **Diagramme...** | Zeigt Diagramme an, die die zeitliche Aktivität der Appliance darstellen. Obwohl Sie ein Protokoll nach Klicken auf "Bearbeiten" abwählen können, überwacht die Appliance den Verkehr weiterhin. |

## Lastenausgleich

HINWEIS: Dieser Abschnitt ist nur auf einer Cluster-Master-Appliance oder einem Management-Blade (auf einem Content Security Blade Server) verfügbar.

Tabelle 7: Lastenausgleich – Optionsbeschreibungen

| Option | Beschreibung |
|---|---|
| **E-Mail** | Wenn Sie hierauf klicken, zeigt die Anzeige Nachrichten pro Stunde (E-Mail) an. |
| **Nachrichten pro Stunde (E-Mail)** | Zeigt den durchschnittlichen Durchsatz des Clusters auf der Grundlage der alle paar Minuten vorgenommenen Messungen. Wenn ein Cluster doppelt so viele Scan-Appliances umfasst, verdoppelt sich der Durchsatz fast. Zusätzliche Verwaltungsaktivitäten beanspruchen ebenfalls Verarbeitungsleistung. |
| **Status** | Zeigt den Status des Geräts an:<br>• – Normaler Betrieb<br>• – Erfordert Aufmerksamkeit<br>• – Erfordert sofortige Aufmerksamkeit |
| **Typ des Scan-Geräts** | Zeigt den Typ des Scan-Geräts an:<br>• – Cluster-Master<br>• – Cluster-Failover |

| Option | Beschreibung |
|---|---|
| | • – Email Security Appliance |
| **Name** | Zeigt den konfigurierten Namen der Appliance an. |
| **Status** | Zeigt den aktuellen Status der einzelnen Appliances an:<br>• **Netzwerk** – Mit dem Netzwerk verbunden.<br>• **Redundant** – Das Cluster-Failover-Gerät arbeitet derzeit nicht, übernimmt jedoch, falls die Master-Cluster-Appliance fehlschlägt.<br>• **Installieren** – Installieren der Software.<br>• **Synchronisieren** – Synchronisieren mit dem Cluster-Master.<br>• **Starten** – Neustart wird durchgeführt.<br>• **Herunterfahren** – Das Gerät wird heruntergefahren.<br>• **Falsch konfiguriert** – Die Konfigurationsdatei ist fehlerhaft.<br>• **Nicht konfiguriert** – Nicht für den Lastenausgleich konfiguriert.<br>• **Deaktiviert** – Durch den Benutzer deaktiviert.<br>• **Fehlgeschlagen** – Nicht mehr im Netzwerk. Es wurde kein "Heartbeat" erkannt.<br>• **Fehler** – Auf dieser Appliance wurde ein Fehler festgestellt.<br>• **Frühere Version** – Nicht mit dem Lastenausgleich kompatibel. |
| **Auslastung** | Zeigt die durchschnittliche Systemauslastung während eines Zeitraums von fünf Minuten an. |
| **Aktiv** | Zeigt die Anzahl an aktiven Verbindungen für jede Appliance an. Die Zeile für den Cluster-Master zeigt die Gesamtzahl für alle Appliances an. |
| **Verbindungen** | Zeigt die Anzahl an Verbindungen an, die von den einzelnen Appliance verarbeitet wurden, seit die Zähler zum letzten Mal zurückgesetzt wurden. |
| **Informationen zur Komponentenversion** | Zeigt die Versionen der Anti-Spam- und Antiviren-DAT-Dateien. Wenn die Appliances auf dem aktuellen Stand sind, stimmen die Versionsnummern überein. Während der Aktualisierung können die Werte voneinander abweichen. Um weitere Informationen anzuzeigen, bewegen Sie den Mauszeiger über den Text, und warten Sie, bis ein gelbes Kästchen angezeigt wird. |

## Zählerverhalten

Alle Zähler lösen für jede Erkennung einmal aus. Wenn beispielsweise eine Nachricht zwei Anhänge hat, die beide infizierte Inhalte enthalten, wird der **Virenzähler** um zwei erhöht. Die Informationen in der folgenden Tabelle gelten, sofern nicht anders angegeben, für SMTP- und POP3-Statistiken.

Tabelle 8: Zählerverhalten

| Zähler | Verhalten |
|---|---|
| **Nachrichten** | Der **SMTP-Zähler** wird in folgenden Fällen um eins erhöht:<br>• Wenn eine TCP-Verbindung zum SMTP-Port auf der Appliance hergestellt wird |

| Zähler | Verhalten |
|---|---|
| | • Ab dem zweiten <MAIL FROM>-Befehl, wenn mehrere E-Mails in derselben SMTP-Konversation empfangen werden<br>Der **POP3-Zähler** wird für jede Nachricht, die von der Appliance heruntergeladen wird, um eins erhöht. |
| **Sichere Nachrichten** | Wird in den folgenden Fällen um eins erhöht:<br>• Wenn ein STARTTLS-Befehl über den Standard-SMTP-Port ausgegeben wird<br>• Wenn die Appliance die TLS-Konversation abfängt, ab dem zweiten <MAIL FROM>-Befehl, wenn mehrere E-Mails in derselben SMTP-Konversation empfangen werden<br>• Wenn Nachrichten über SMTPS gesendet werden |
| **Blockierte Verbindungen** | Wird für jedes SYN-Paket um eins erhöht, das von einer IP-Adresse stammt, die eine "Ablehnen, schließen und verweigern (Blockieren)"-Aktion ausgelöst hat. Die RBL-Suchfunktion (Realtime Blackhole List) ist so konfiguriert, dass diese Aktion standardmäßig für die nächsten zehn Minuten ausgeführt wird. |
| **Viren, PUPe, Compliance und Data Loss Prevention** | Wird für jede Erkennung um eins erhöht. Wenn beispielsweise eine Nachricht zwei Anhänge hat, die beide infizierte Inhalte enthalten, wird der **Virenzähler** um zwei erhöht. |
| **Spam und Phishing** und **Absenderauthentifizierung** | Wird für jede Nachricht, die den Scanner auslöst, um eins erhöht |
| **Sonstige** | Wird für jede Erkennung um eins erhöht. Gilt für Nachrichten, die aufgrund ihrer Größe gefiltert werden, Nachrichten, die bei Anti-Relay- und Directory-Harvest-Prüfungen durchfallen, und Nachrichten, die beschädigten Inhalt, geschützten Inhalt, verschlüsselten Inhalt oder signierten Inhalt enthalten. |

HINWEIS: Aufgrund der Weise, wie das Dashboard Zähler aggregiert, gibt es eine kleine Differenz zwischen den Informationen, die im Dashboard angezeigt werden, und denen, die in einem geplanten Bericht enthalten sind.

### Information zu Statistiken, die in der Liste "E-Mail-Warteschlangen" angezeigt werden

Diese Informationen gelten für die Warteschlangen **In der Warteschlange**, **Isoliert** und **Anfragen für Entlassen aus Quarantäne**:

- Wenn eine Nachricht an zwei Empfänger gesendet und in die Zustellungswarteschlange gestellt wird (beispielsweise, weil der weiterführende MTA ausgefallen ist), gilt Folgendes:
  - Die Anzahl der Elemente in der Warteschlange ist 1, da die Appliance eine Nachricht empfangen hat.
  - Die Anzahl der Empfänger ist 2, da die Nachricht zwei Empfänger hat.

  HINWEIS: Wenn Sie auf den Link **In der Warteschlange** klicken, werden zwei Elemente angezeigt, da für jeden Empfänger eine Nachricht vorhanden ist.
- Wenn zwei Nachrichten an einen Empfänger gesendet und in die Zustellungswarteschlange gestellt werden (beispielsweise, weil der weiterführende MTA ausgefallen ist), gilt Folgendes:
  - Die Anzahl der Elemente in der Warteschlange ist 2, da die Appliance zwei Nachrichten empfangen hat.

- Die Anzahl der Empfänger ist 2, da jede Nachricht einen Empfänger hat.

HINWEIS: Wenn Sie auf den Link **In der Warteschlange** klicken, werden zwei Elemente angezeigt.

**Vorgehensweise – Deaktivieren des Warnhinweises "McAfee Global Threat Intelligence-Feedback deaktiviert"**

Die Appliance zeigt standardmäßig eine Warnmeldung an, wenn das McAfee Global Threat Intelligence-Feedback (GTI-Feedback) nicht aktiviert ist, da es von McAfee als bewährte Vorgehensweise angesehen wird, diese Form der Kommunikation zu aktivieren.

1. Wählen Sie im Appliance-Dashboard im Bereich "Systemstatus" die Option **Bearbeiten** aus.
2. Deaktivieren Sie **Einen Warnhinweis anzeigen, wenn McAfee GTI-Feedback nicht aktiviert ist**.
3. Klicken Sie auf **OK**.

# Testen der Konfiguration

Diese Informationen beschreiben, wie Sie testen können, ob die Email Security Appliance (VMtrial) nach der Installation ordnungsgemäß funktioniert. Wenn Sie sich zum ersten Mal bei der Appliance anmelden, wird empfohlen, den Bereich "Systemstatus" des Dashboards zu überprüfen, in dem empfohlene Konfigurationsänderungen angezeigt werden.

## Testen der Verbindung

Gehen Sie wie nachfolgend beschrieben vor, um die grundlegende Verbindungsfähigkeit zu bestätigen. VMtrial prüft, ob es mit dem Gateway kommunizieren und Server sowie DNS-Server aktualisieren kann. Außerdem wird bestätigt, dass der Name und der Domänenname gültig sind.

### Vorgehensweise

1. Öffnen Sie die Seite **Systemtests** mit einer der folgenden Methoden:
   - Wählen Sie im Bereich "Tasks" des Dashboards die Option **Systemtests ausführen**.
   - Wählen Sie in der Navigationsleiste die Option **Fehlerbehebung**.
2. Klicken Sie auf die Registerkarte **Tests**.
3. Klicken Sie auf **Tests starten**. Verifizieren Sie, dass jeder Test positiv ist.

## Aktualisieren der DAT-Dateien

Sobald Sie die Konfigurationskonsole ausgefüllt haben, versucht VMtrial, alle aktivierten Scanner zu aktualisieren. Gehen Sie wie nachfolgend beschrieben vor, um sicherzustellen, dass die Email Security Appliance (VMtrial) über die aktuellsten Erkennungsdefinitionsdateien (DAT) verfügt.

Im Rahmen der Verwendung von VMtrial können Sie einzelne Arten von Definitionsdateien aktualisieren sowie die standardmäßig geplanten Aktualisierungen an Ihre Anforderungen anpassen.

### Vorgehensweise

1. Öffnen Sie die Seite **Aktualisierungen** mit einer der folgenden Methoden:
   - Wählen Sie im Bereich **Systemstatus** des Dashboards die Option **Aktualisierungen**.
   - Wählen Sie **System | Komponentenverwaltung | Aktualisierungsstatus**.
2. Wenn Sie alle DAT-Dateien aktualisieren möchten, klicken Sie neben der Antiviren-Modul-Komponente auf **Jetzt aktualisieren**.

## Testen von E-Mail-Verkehr und Virenerkennung

Gehen Sie wie nachfolgend beschrieben vor, um zu überprüfen, ob E-Mail-Verkehr erfolgreich durch VMtrial geleitet wird und Bedrohungen ordnungsgemäß identifiziert werden. Wir verwenden die EICAR-Testdatei, eine harmlose Datei, die eine Virenerkennung auslöst.

### Vorgehensweise

1. Senden Sie eine E-Mail von einem externen E-Mail-Konto (wie Hotmail) an einen internen Posteingang, und vergewissern Sie sich, dass die E-Mail angekommen ist.
2. Sehen Sie sich im Dashboard den Bereich **E-Mail-Erkennungen** an. Aus der Liste für das Protokoll, das Sie zum Versenden der Nachricht verwendet haben, sollte hervorgehen, dass eine Nachricht empfangen wurde.
3. Kopieren Sie die folgende Zeile in eine Datei, und achten Sie dabei darauf, dass Sie keine Leerzeichen oder Zeilenumbrüche hinzufügen:

   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARDANTIVIRUS-TEST-FILE!$H+H*
4. Speichern Sie die Datei unter dem Namen EICAR.COM.
5. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine Nachricht mit der Datei EICAR.COM als Anhang, und senden Sie die Nachricht an einen internen Posteingang.
6. Kehren Sie zum Dashboard zurück, und sehen Sie sich den Bereich **E-Mail-Erkennungen** an. Sie sollten sehen, dass ein Virus erkannt wurde.
7. Löschen Sie die Nachricht, wenn Sie das Testen Ihrer Installation abgeschlossen haben, damit ahnungslose Benutzer keinen Schreck bekommen.

## Testen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um einen "General Test mail for Unsolicited Bulk Email" (Allgemeinen Test auf unerwünschte Bulk-E-Mails – GTUBE) auszuführen, mit dem geprüft wird, ob eingehender Spam erkannt wird.

### Vorgehensweise

1. Erstellen Sie von einem externen E-Mail-Konto (SMTP-Client) aus eine neue E-Mail.
2. Kopieren Sie den folgenden Text in den Nachrichtenteil der E-Mail:

   XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARDANTI-UBE-TEST-EMAIL*C.34X

   Vergewissern Sie sich, dass Sie keine Leerzeichen oder Zeilenumbrüche eingeben.
3. Senden Sie die neue E-Mail an eine interne Posteingangsadresse. Die Software scannt die Nachricht, erkennt sie als Junk-E-Mail und verarbeitet sie entsprechend. Der GTUBE-Test hat Vorrang vor Blacklists und Whitelists.

# Erkunden der VMtrial-Funktionen

In diesem Abschnitt finden Sie Vorgehensweisen zur Demonstration der Scan-Funktionen von Email Security Appliance (VMtrial). Sie werden detailliert durch das Erstellen und Testen einiger Beispielrichtlinien geführt und erfahren, wie Sie die relevanten Berichte generieren.

**Inhalt**


- Vermeiden des Verlusts vertraulicher Daten
- Bearbeiten von isolierten Nachrichten


## Scan-Richtlinien und deren Einfluss auf Ihr Netzwerk

Eine Richtlinie ist eine Zusammenstellung von Einstellungen und Regeln, die Email Security Appliance mitteilen, wie bestimmte Gefahren für Ihr Netzwerk abgewehrt werden sollen. Wenn Sie Echtzeitscan-Richtlinien für Ihr Unternehmen erstellen, müssen Sie Ihre Anforderungen in Ruhe analysieren und planen. Hinweise für die Richtlinienplanung finden Sie in der Online-Hilfe, die über die Produktbenutzeroberfläche aufgerufen werden kann.

## Inhaltsscans unter Verwendung der E-Mail-Compliance-Regeln

Verwenden Sie Compliance-Scans zur Unterstützung der Compliance mit gesetzlichen und betrieblichen Auflagen. Sie können aus einer Bibliothek aus vordefinierten Compliance-Regeln wählen oder eigene Regeln und Wörterbücher für Ihr Unternehmen erstellen.

Compliance-Regeln können hinsichtlich ihrer Komplexität von einem einfachen Auslöser bei der Erkennung eines einzelnen Begriffs in einem Wörterbuch bis hin zum Aufbauen auf und Kombinieren von faktorbasierten Wörterbüchern variieren, die nur auslösen, wenn ein bestimmter Schwellenwert erreicht wird. Mithilfe der erweiterten Funktionen von Compliance-Regeln können Wörterbücher mit den logischen Operationen eines von, alle von oder außer kombiniert werden.

**1** Gehen Sie wie folgt vor, um E-Mail-Nachrichten zu blockieren, die die Richtlinie "Bedrohliche Sprache" verletzen:

- **a** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.
- **b** Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.
- **c** Klicken Sie auf **Neue Regel aus Vorlage erstellen**, um den Assistenten für die Regelerstellung zu öffnen.
- **d** Wählen Sie die Richtlinie **Zulässige Nutzung - Bedrohliche Sprache** aus, und klicken Sie auf **Weiter**.
- **e** Sie können den Namen der Regel optional ändern. Klicken Sie anschließend auf **Weiter**.
- **f** Ändern Sie die primäre Aktion in **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **Fertig stellen**.
- **g** Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

**2** Gehen Sie wie folgt vor, um eine einfache benutzerdefinierte Regel zum Blockieren von E-Mail-Nachrichten zu erstellen, die Sozialversicherungsnummern enthalten

- **a** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

**b** Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

**c** Klicken Sie auf **Neue Regel erstellen**, um den **Assistenten für die Regelerstellung** zu öffnen.

**d** Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

**e** Geben Sie im **Suchfeld** sozial ein.

**f** Wählen Sie das Wörterbuch **Sozialversicherungsnummer** aus, und klicken Sie zweimal auf **Weiter**.

**g** Wählen Sie die Aktion **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **Fertig stellen**.

**3** Gehen Sie wie folgt vor, um eine komplexe Regel zu erstellen, die auslöst, wenn sowohl Wörterbuch A als auch Wörterbuch B erkannt werden, jedoch nicht, wenn darüber hinaus auch Wörterbuch C erkannt wird.

**a** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

**b** Klicken Sie im Dialogfeld **Standard-Compliance-Einstellungen** auf **Ja**, um die Richtlinie zu aktivieren.

**c** Klicken Sie auf **Neue Regel erstellen**, um den Assistent für die Regelerstellung zu öffnen.

**d** Geben Sie einen Namen für die Regel ein, und klicken Sie auf **Weiter**.

**e** Wählen Sie zwei Wörterbücher aus, die in die Regel aufgenommen werden sollen, und klicken Sie auf **Weiter**.

**f** Wählen Sie in der Ausschlussliste ein Wörterbuch aus, das Sie von der Regel ausschließen möchten.

**g** Wählen Sie die Aktion aus, die ausgeführt werden soll, wenn die Regel ausgelöst wird.

**h** Wählen Sie im Dropdown-Feld **Und bedingt** die Option **Alle** aus, und klicken Sie auf **Fertig stellen**.

**4** Gehen Sie wie folgt vor, um ein neues Wörterbuch zu einer vorhandenen Regel hinzuzufügen:

**a** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

**b** Erweitern Sie die Regel, die Sie bearbeiten möchten.

**c** Wählen Sie **Wörterbuch hinzufügen**.

**d** Wählen Sie das neue Wörterbuch aus, das Sie hinzufügen möchten, und klicken Sie auf **OK**.

**5** Gehen Sie wie folgt vor, um eine "Unzufriedenheit"-Regel zu konfigurieren, die mit einem niedrigen Schwellenwert überwacht wird und bei einem hohen Schwellenwert blockiert:

**a** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

**b** Klicken Sie auf **Neue Regel erstellen**, geben Sie einen Namen für die Regel ein, beispielsweise Unzufriedenheit - Niedrig, und klicken Sie auf **Weiter**.

**c** Wählen Sie das Wörterbuch "Unzufriedenheit" aus, und geben Sie unter "Schwelle" den Wert 20 ein.

**d** Klicken Sie auf **Weiter** und anschließend erneut auf **Weiter**.

**e** Akzeptieren Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Standardaktion.

**f** Klicken Sie auf **Fertig stellen**.

**g** Wiederholen Sie die Schritte 2 bis 4, um eine weitere neue Regel zu erstellen. Nennen Sie diese jedoch Unzufriedenheit – Hoch, und weisen Sie ihr den Schwellenwert 40 zu.

**h** Wählen Sie unter **Wenn die Compliance-Regel ausgelöst wird** die Option **Daten akzeptieren und anschließend verwerfen (Blockieren)** aus.

**i** Klicken Sie auf **Fertig stellen**.

**j** Klicken Sie auf **OK**, und übernehmen Sie die Änderungen.

**6** Gehen Sie wie folgt vor, um den Schwellenwert zu bearbeiten, der einer vorhandenen Regel zugeordnet ist. Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch "Vergütung und Leistungen":

**a** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

**b** Erweitern Sie die Regel, die Sie bearbeiten möchten, und wählen Sie anschließend das Symbol Bearbeiten neben dem Wörterbuch aus, dessen Faktor Sie ändern möchten.

**c** Geben Sie unter "Schwellenwert für Wörterbuch" den Faktor ein, bei dem die Regel ausgelöst werden soll, und klicken Sie auf **OK**.

**7** Gehen Sie wie folgt vor, um den Faktorbeitrag eines Wörterbuchbegriffs zu beschränken. Bei dieser Vorgehensweise wird davon ausgegangen, dass Ihre Regel ein Wörterbuch enthält, das die Aktion basierend auf einem Schwellenwert auslöst, beispielsweise das Wörterbuch "Vergütung und Leistungen". Bei solchen Wörterbüchern können Sie beschränken, wie oft ein Begriff zum Gesamtfaktor beitragen kann.

**a** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinien**, und wählen Sie **Compliance**.

**b** Erweitern Sie die Regel, die Sie bearbeiten möchten, und klicken Sie anschließend auf das Symbol "Bearbeiten" neben dem Wörterbuch, dessen Faktor Sie ändern möchten.

**c** Geben Sie unter **Max. Begriffsanzahl** die maximale Anzahl an Vorkommnissen eines Begriffs an, die zum Gesamtfaktor beitragen sollen.

# Vermeiden des Verlusts vertraulicher Daten

Gehen Sie wie nachfolgend beschrieben vor, um das Versenden eines vertraulichen Finanzdokuments aus Ihrem Unternehmen heraus zu blockieren.

## Vorgehensweise

**1** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Registrierte Dokumente**, und erstellen Sie die Kategorie Finanzen.

**2** Navigieren Sie zu **E-Mail | E-Mail-Richtlinien | Scan-Richtlinie**, und wählen Sie die **Data Loss Prevention**-Richtlinie aus.

**3** Klicken Sie im Dialogfeld **Standardeinstellungen für Data Loss Prevention** auf **Ja**, um die Richtlinie zu aktivieren.

**4** Klicken Sie auf **Neue Regel erstellen**, wählen Sie die Kategorie "Finanzen" aus, und klicken Sie auf **OK**, damit die Kategorie in der Liste "Regeln" angezeigt wird.

5 Wählen Sie die der Kategorie zugeordnete Aktion aus, ändern Sie die primäre Aktion in **Daten akzeptieren und anschließend verwerfen (Blockieren)**, und klicken Sie auf **OK**.

6 Klicken Sie erneut auf **OK**, und übernehmen Sie die Änderungen.

# Bearbeiten von isolierten Nachrichten

Gehen Sie wie nachfolgend beschrieben vor, um nach E-Mails zu suchen, die aufgrund von Compliance-Problemen isoliert wurden, und geben Sie die Nachricht an den vorgesehenen Empfänger frei.

### Vorgehensweise

1 Klicken Sie auf **E-Mail | Nachrichtensuche**.

2 Wählen Sie **Isoliert** in der Dropdown-Liste **Nachrichtenstatus** aus.

3 Klicken Sie auf **Suchen/Aktualisieren**.

Alle isolierten Nachrichten werden im unteren Bereich der Seite angezeigt.

4 Um die E-Mails zu finden, die aufgrund von Compliance-Problemen in Quarantäne verschoben wurden, wählen Sie **Compliance** in der Dropdown-Liste **Kategorie** aus.

5 Klicken Sie auf **Suchen/Aktualisieren**.

Der untere Bereich des Bildschirms wird aktualisiert, um nur die Nachrichten anzuzeigen, die aufgrund von Compliance-Problemen isoliert wurden.

6 Um eine E-Mail anzuzeigen, die aufgrund von Compliance-Problemen in Quarantäne verschoben wurde, wählen Sie die entsprechende isolierte Nachricht mit Hilfe des Kontrollkästchens links auf der Seite aus.

7 Klicken Sie auf **Nachricht anzeigen**.

Die ausgewählte Nachricht wird in einem neuen Fenster angezeigt. In diesem Fenster können Sie den Inhalt der E-Mail lesen. Außerdem können Sie alternativ die detaillierten Informationen des E-Mail-Headers anzeigen.

8 Klicken Sie auf **Ausgewählte Elemente aus Quarantäne entlassen**, um die isolierte E-Mail freizugeben.

Die ausgewählte E-Mail wird aus der Quarantäne entlassen.

HINWEIS: E-Mails mit infiziertem Inhalt können nicht aus der Quarantäne entlassen werden, da dies Schäden auf Ihren Systemen verursachen könnte.

# Überwachen der Spam-Erkennung

Gehen Sie wie nachfolgend beschrieben vor, um die Spam-Erkennungsrate mit der standardmäßigen SMTP-Spam-Erkennungsrichtlinie überwachen. Sobald Sie die Konfigurationskonsole ausgeführt haben, funktionieren diese Einstellungen und schützen Ihr Netzwerk und Ihre Benutzer vor unerwünschten Spam-Nachrichten. Eine ausführlichere Erläuterung der Einstellungen finden Sie in der Online-Hilfe, die über die Benutzeroberfläche aufgerufen werden kann.

Standardmäßig gilt für Email Security Appliance (VMtrial):

- Sie blockiert Phishing-Nachrichten.

- Sie markiert Nachrichten mit einer Einstufung von mindestens fünf als Spam.
- Sie verwirft Spam-Nachrichten mit einer Einstufung von mindestens zehn.
- Die Absenderauthentifizierung ist aktiviert.

Mithilfe dieser Standardeinstellungen erkennt VMtrial mehr als 98 Prozent aller Spam-Nachrichten.

HINWEIS: Die Einstellungen für die Absenderauthentifizierung umfassen die E-Mail-Reputation von McAfee Global Threat Intelligence. Wenn ein Absender die E-Mail-Reputation-Prüfung von McAfee Global Threat Intelligence nicht besteht, weist VMtrial die E-Mail zurück, beendet die Verbindung und lässt die IP-Adresse des Absenders nicht mehr zu. Die IP-Adresse des Absenders wird zu einer Liste blockierter Verbindungen hinzugefügt und automatisch zehn Minuten lang auf Kernel-Ebene blockiert (die standardmäßige Blockierdauer kann geändert werden). Im Bereich **E-Mail-Erkennungen** des Dashboards wird die Anzahl der blockierten Verbindungen angezeigt.

### Vorgehensweise

1. Wählen Sie im Bereich **Scan-Richtlinien** des Dashboards die Option **SMTP | Standardrichtlinie**, um die Standardeinstellungen für die Spam-Erkennung anzuzeigen.
2. Vergewissern Sie sich, dass Spam-Nachrichten ordnungsgemäß identifiziert werden, indem Sie eine Nachricht VMtrial passieren lassen, bei der die Einstellungen zur Spam-Erkennung ausgelöst werden.
3. Wenn Sie die Erkennungsrate überwachen möchten, kehren Sie zum Dashboard zurück, und betrachten Sie den Bereich **E-Mail-Erkennungen**.
   Die Zahl für **Spam und Phishing** und für **Absenderauthentifizierung** wird hochgezählt. Die Zahl für die Absenderauthentifizierungserkennungen beinhaltet die Anzahl der Absender, die die E-Mail-Reputation-Prüfung von McAfee Global Threat Intelligence nicht bestanden haben. **E-Mail-Diagramme** bietet eine graphische Darstellung der Daten.
4. Wenn Sie einen Bericht über die E-Mail-Aktivität erhalten möchten, gehen Sie zu **Tasks**, und wählen Sie **Bevorzugte E-Mail-Berichte anzeigen**.
5. Sehen Sie sich den Bericht **Blockiert (heute)** und den Bericht **Häufigste Spam-Absender (heute)** an.

# Ausführen von VMtrial auf dem VMware Server im Betriebsmodus "Transparent"

Gehen Sie wie nachfolgend beschrieben vor, um VMtrial so einrichten, dass es in einem der transparenten Betriebsmodi betrieben wird.

Die standardmäßige VMware Server-Konfiguration reicht aus, um VMtrial im Modus "Expliziter Proxy" der Email Security Appliance (VMtrial) auszuführen.

HINWEIS: Um Email Security Appliance (VMtrial) im Modus "Transparenter Router" auszuführen, benötigen Sie zwei physische Netzwerkadapter.

### Vorgehensweise

1. Verbinden Sie die Netzwerkschnittstellenkarten (Network Interface Cards, NIC) von VMtrial über ein virtuelles Netzwerk im Bridge-Modus mit der physischen Netzwerkschnittstelle des Host-Computers, um die zweite Bridge-Schnittstelle zu erstellen:

- Öffnen Sie unter VMware Server 1.0, das unter dem Betriebssystem Microsoft Windows ausgeführt wird, die VMware Server-Konsole, und wählen Sie **Host | Virtual Network Settings** (Host | Virtuelle Netzwerkeinstellungen).
- Öffnen Sie auf VMware Server 2.0 den Virtual Network Editor (**Start | VMware | VMware Server | Manage Virtual Networks**) (Start | VMware | VMware-Server | Virtuelle Netzwerke verwalten). Wenn Sie das Betriebssystem Microsoft Windows Vista verwenden, klicken Sie mit der rechten Maustaste auf **Manage Virtual Networks** (Virtuelle Netzwerke verwalten), und wählen Sie **Run as administrator** (Als Administrator ausführen).
- Öffnen Sie unter Linux eine Shell, und führen Sie das Skript vmware-config.pl aus. Befolgen Sie dann die Anweisungen zum Networking Setup (Netzwerk-Setup). Bestätigen Sie, dass Sie eine zweite Bridge-Schnittstelle erstellen möchten.

**2** Wählen Sie auf der Registerkarte **Host Virtual Network Mapping** (Host für virtuelle Netzwerkzuordnung) den physischen Netzwerkadapter für **VMnet2** und für **VMnet3** aus.

**3** Übernehmen Sie die Änderungen.

**4** Klicken Sie in der Liste **Inventory** (Inventar) mit der rechten Maustaste auf das Appliance-Image, und klicken Sie dann auf **Settings** (Einstellungen).

**5** Wählen Sie im Fenster **Device** (Gerät) **Ethernet**.

**6** Wählen Sie als Netzwerkverbindung **Custom** (Benutzerdefiniert) aus.

**7** Wählen Sie VMtrial VMnet2/3 in Abhängigkeit davon aus, auf welcher Schnittstelle LAN1 für die virtuelle Appliance erstellt werden soll.

**8** Wählen Sie die virtuelle Schnittstelle für Ethernet 2/LAN2.

**9** Übernehmen Sie die Änderungen.

**10** Starten Sie VMtrial.

**11** Konfigurieren Sie VMtrial als transparenten Router.

700-2968A15

McAfee®